REMARKS

The above amendments and following remarks are submitted as a preliminary amendment accompanying a Request for Continued Examination filed on even date. Having addressed all objections and grounds of rejection presented by the Examiner in his Advisory Action provided to Applicants by Facsimile on January 7, 2004, claims 1-20, being all the pending claims, are now deemed in condition for allowance. Entry of these amendment and reconsideration to that end is respectfully requested.

The Examiner has continued his objection to the specification notwithstanding the arguments made by Applicants in their previous submission. The undersigned wishes to apologize for any misunderstandings in this regard and would agree to any reasonable modifications which might be suggested. However, having again reviewed Applicants' specification and drawings, the undersigned believes that Applicants' invention is completely and unambiguously taught therein.

Specifically, the disclosure "relates to enhancements for providing secure access to data base management systems via Internet user terminals[1]". "There are two basic problems with

---

[1]See specification page 3, lines 4-5.

permitting Internet access to a proprietary data base. The first is a matter of security. Because the Internet is basically a means to publish information, great care must be taken to avoid intentional or inadvertent access to certain data by unauthorized Internet users. In practice this is substantially complicated by the need to provide various levels of authorization to Internet users to take full advantage of the technique. For example, one might have a first level involving no special security features available to any Internet user. A second level might be for specific customers, whereas a third level might be authorized only for employees. One or more fourth levels of security might be available for officers or others having specialized data access needs.

Existing data base managers have security systems, of course. However, because of the physical security with a proprietary system, a certain degree of security is inherent in the limited access. On the other hand, access via the Internet is virtually unlimited which makes the security issue much more acute. Current day security systems involving the world wide web involve the presentation of a user-id and password. Typically, this user-id and password either provides access or denies access in a binary fashion.[2]" "The practical security problem is to

---

[2]See specification at page 4, line 21, through page 5, line 14.

provide individualized access to secure portions of a data base wherein the user employs dialog accessing techniques. In the past, the logic for regulating such secure access was lodged within the logic to honor the service request. This results in duplication of effort and non-compatibility over a range of service request types.[3]"

Those of skill in the art will readily appreciate that a user-id and a password are just numbers. In the prior art, these numbers are utilized by a system at a particular time to uniquely identify a user. However, as is readily known to "hackers", if a valid number(s) is presented to the system at the proper time(s) and in the proper format(s), the system will assume that it has successfully identified a particular user regardless of the means of generation of the number.

"In order to permit any such access [i.e., secure and authorized], the present invention has a security feature that requires a user to sign on with a UserID and Password when secured services are requested.[4]" So far, this is similar to the prior art, except that it only identifies the specific user to the terminal at a specific site rather than to the data base management system over the Internet. "This invention will

---

[3]See specification at page 6, lines 15-18.

[4]See specification at page 7, lines 9-11.

provide a new SignOn capability which allows for site-specific data to be used to identify a user. The site-specific data is converted to a valid UserID/Password by a User Validation service implemented by a site.[5]" In other words, the physical site obtains approval from the data base management system for access to secure data quite apart from the identity of the individual user. It should be apparent that without *a priori* notification and as long as the data base management system receives the valid number(s) at the appropriate time(s) and in the appropriate format(s), the data base management system will not be able to distinguish between the identification of a specific individual user and the identification of a specific physical site.

Though not exhaustive, the specification provides some ideas about how one would utilize the combination of user identification and site identification. "{S}such a security system should provide multiple levels of access to accommodate a variety of authorized user categories. Site specific profiles may offer only limited or no access to sensitive data when the user terminal site is not particularly secure. These features can be effectively combined with physical security procedures to provide many specialized security profiles. Each individual service within an ASP may be validated. Other solutions must

---

[5]See specification at page 7, lines 11-13.

still transmit sign on over the network for each service. Even though such transmissions may be encrypted or sent over a secure connection, they can still be susceptible to being accessed and decrypted by malicious users.[6]" In other words, a person may be permitted access to very sensitive data in his/her office but not from a lap top computer in an airline terminal.

Implementation becomes relatively straightforward. "This invention will provide a new SignOn capability which allows for site-specific data to be used to identify a user. The site-specific data is converted to a valid UserID/Password by a User Validation service implemented by a site. This feature requires a site to implement a site-user. The site must also implement a User Validation service. This service will return data in a pre-defined format so that it can be processed.[7]" In other words, the system generates a valid UserID/Password which identifies the physical site, rather than the individual user. It is assumed that other security procedures, such as physical security, prevents misuse of a specific site-identified UserID/Password.

In support of his objection, the Examiner states:

> The objection to the specification stems from the fact that there are three different UserID/Passwords, which

---

[6]See specification at page 7, line 19, through page 8, line 4.

[7]See specification at page 7, lines 11-15.

> are treated differently, yet are not distinguished from each other in the specification.

This statement is factually incorrect. It appears that the Examiner really means that there are UserID/Passwords that are generated in different ways, which are treated similarly. As explained above, the UserID/Password is just a number(s). Once validly generated and presented at the proper time(s) and in the proper format(s), UserID/Passwords are indistinguishable and therefore handled similarly regardless of the details of generation and entry into the system. This is a key point in terms of the invention. The system provides the same treatment for a UserID/Password which uniquely identifies a user ss for a UserID/Password which uniquely identifies a physical site.

The Examiner concludes his argument regarding the UserID/Password by stating:

> Thus, when referring to a UserID/Password, it is unclear to the reader which UserID/Password is being referred to.

That is precisely the point. A UserID/Password is a number. The number is exactly the same whether assigned to uniquely identify a particular user or generated by the system to uniquely identify a physical site. There is no difference.

In addressing the term "User Validation Service", the Examiner states:

> Similarly, there seem to be two different User Validation Services, which operate upon different data,

> yet are not distinguished from each other in the specification, which makes it unclear to the reader which User Validation Service is being referred to.

A quick search of the specification will reveal that the term "User Validation Service" is only utilized twice on page 7 and states:

> The site-specific data is converted to a valid UserID/Password by a User Validation service implemented by a site. This feature requires a site to implement a site-user. The site must also implement a User Validation service. This service will return data in a pre-defined format so that it can be processed.

The term is utilized again on page 8 stating:

> The UserValidation service is used to convert site specific user validation data to a UserID and Password.

It is simply not understood how the Examiner could find these three uses of the term "UserValidation service to be ambiguous.

Additionally, the Examiner has exhibited some confusion with regard to whether a UserID/Password could be transferred over the Internet. In the preferred system, access is granted by both verification of a specific user (as in the prior art) and verification of a specific physical site. The present invention does not change the manner in which the preferred system handles verification of a specific user. It simply adds the ability of the system to provide access by verification of the physical site. In this case, there need by no transfer over the Internet of the specific user identification information.

The Examiner has rejected claims 1-20, being all pending claims, under 35 U.S.C. 112, first paragraph. In partial support of his position, the Examiner cites the specification at page 34, lines 9-12, wherein the service handler requests that a user ID be provided upon a determination that a particular access request involves a security profile. As explained above, whereas this request is made, in response thereto, the service handler may receive a site specific User ID/Password rather than a user specific User ID/Password. As fully understood, the service handler cannot and need not distinguish between these two possibilities. Figs. 13 and 14 provide a more detailed view of the exact process. The rejection on this basis is respectfully traversed, because the service handler request does not specify nor can it determine how the user Id has been generated.

The Examiner is further concerned with the use of the term "special filed" within claims 3, 7, 13, and 17. In response thereto, these claims have been amended to utilize the more general term "portion of the service request", which is directly supported at page 8, line 8. Should the Examiner prefer, Applicants would entertain the suggestion to utilize the more specific "hidden field" of Fig. 14.

With regard to the rejections on the prior art, Applicants now understand that the Examiner has cited a reference (i.e., di Vimercati) for which unsecured data may be transferred upon

request without transfer of a user identifier or other means of authorizing the request. It is now readily apparent that Applicants' claims previously did not limit the transfer requests without user identification to requests for such secure data. As a result, Applicants have herewith amended all pending claims to make it explicit that the claimed transfers are with regard to secure data.

Having thus responded to each objection and ground of rejection, Applicants respectfully request entry of this amendment and allowance of claims 1-20, being the only pending claims.

Respectfully submitted,

Paul S. Germscheid, et al

By their attorney,

Date February 9, 2004

Wayne A. Sivertson
Reg. No. 25,645
Suite 401
Broadway Place East
3433 Broadway Street N.E.
Minneapolis, Minnesota
55413
(612) 331-1464